REMARKS

In the final Office Action[1], the Examiner rejected claims 1-36 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,590,199 by Krajewski, Jr. et al. ("*Krajewski*") in view of U.S. Patent No. 5,005,200 by Fischer ("*Fischer*").

I. Regarding the rejection of claims 1-36 under 35 U.S.C. § 103(a) as being unpatentable over *Krajewski* in view of *Fischer*

Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 1-36 because a *prima facie* case of obviousness has not been established with respect to these claims.

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). M.P.E.P. § 2142, 8th Ed., Rev. 2 (May 2004), p. 2100-128.

A *prima facie* case of obviousness has not been established because, among other things, neither *Krajewski* nor *Fischer*, taken alone or in combination, teach or suggest each and every element recited by Applicant's claims.

Claim 1 recites a method including, for example:

> transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message;

---

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

transmitting the principal-authenticating credentials from the network server to the validation server;

transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;

establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate;

(emphasis added). *Krajewski* does not teach or suggest at least these elements. *Krajewski* discloses a network heterogeneous computer systems that include "at least one user workstation and one authentication server connected to each other through a network" (col. 3, lines 43-45). The user 10 enters a user id 41 into workstation 14 and a request 43 is sent to the KAS 32. A ticket is generated by the KAS 32 and sent to the user workstation 14. The user enters a password 42 which is sent to the smart card 30 and decrypted (col. 5, line 65 - col. 6, line 9). If the user 10 wishes to access a specific system service 20, the user presents the service ticket and associated authenticator 51 to "the ticket granting service running on the KAS 32 to request a ticket for the desired system service 20" (col. 6, lines 10-14). The ticket granting service generates and sends an appropriate ticket and server session key 52 to the user's workstation. The key is decrypted and smart card 30 encrypts an appropriate authenticator for the desired ticket service and the user may then obtain access to service 20 (col. 6, lines 18-28).

The Examiner states that system service 20 constitutes the claimed network server and *Krajewski*'s KAS 32 constitutes the claimed validation center (Office Action at page 4). However, this is not correct. In *Krajewski*, the user sends information for a ticket to KAS 32, and KAS 32 generates the user's ticket (col. 6, lines 11-16). The user

presents this ticket to the system service 20 to obtain access. Any credentials that may exist in *Krajewski* are transmitted from the user 10 to KAS 32 and to the system service 20 (col. 5, line 65 - col. 6, line 5 and col. 6, lines 24-28). System service 20 does not interact with KAS 32. Therefore, *Krajewski* does not teach "transmitting the principal-authenticating credentials from the network server to the validation server", as recited in claim 1. Furthermore, *Krajewski* does not teach "transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials", at least because KAS 32 interacts with user 10, not system service 20.

The Examiner also states that the Kerebos server corresponds to the claimed destination server (Office Action at page 4). Applicant respectfully disagrees. *Krajewski* disclose a system for user access to a specific system service. Kerebos is a protocol for developing a secure login. Kerebos uses an authentication server (KAS 32). Therefore, because the only server associated with Kerebos is KAS 32, which the Examiner correlates to the claimed validation server, Kerebos cannot be relied upon to teach the claimed destination server as stated by the Examiner (Office Action at page 4). Even assuming, absent any teaching in the prior art, that Kerebos includes another server that is separate and distinct from KAS 32, Kerebos does not exchange data with the system service 20. As previously stated, KAS 32 interacts with the user 10 and the user 10 interacts with the system service 20. Therefore, *Krajewski* does not teach "exchanging data between the network server and the destination server based on the digital certificate", as further recited in claim 1.

The Examiner correctly notes that *Krajewski* does not teach "establishing a secure connection for exchanging data between the client and the network server and establishing a second secure connection for exchanging data between the network server and the destination server or issuing a digital certificate to a network server" (Office Action at page 5). However, the Examiner relies on *Fischer* to teach this limitation.

Fischer does not cure the deficiencies of *Krajewski*. *Fischer* discloses the creation of a "digital message which contains the claimant's public key and the name of the claimant" (col. 3, lines 53-55). A digital message is sent with a digital signature to ensure the proper authority (col. 3, lines 58-64). However, transmitting a digital message with a digital signature, as in *Fischer*, does not constitute "transmitting the principal-authenticating credentials from the network server to the validation server", "transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials", and "exchanging data between the network server and the destination server based on the digital certificate", as recited in claim 1.

In addition, the references themselves contain no suggestion or motivation to modify or combine them. *Krajewski* discloses "at least one user workstation and one authentication server connected to each other through a network" (col. 3, lines 43-45). This authentication allows the user to access a networked service. In contrast, *Fischer* discloses public key encryption and decryption to ensure the integrity of an electronic message (col. 3, lines 35-64). One of ordinary skill would not have been motivated to

combine authenticating user access to a networked service with data encryption for transmitting electronic messages.

Furthermore, one skilled in the art would only arrive at the present claimed invention by consulting Applicant's disclosure, yet "[t]he teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." M.P.E.P § 2142, internal citations omitted. Relying on the Applicants' own disclosure in an attempt to provide some teaching or suggestion to combine *Krajewski* and *Fischer* constitutes improper hindsight reasoning.

Accordingly, *Krajewski* and *Fischer* fail to establish a *prima facie* case of obviousness with respect to claim 1, at least because the references fail to teach each and every element of the claim. Claims 2-22 depend from claim 1 and are thus also allowable for at least the same reasons as claim 1.

Independent claims 23, 24, 29, and 36, though of different scope from claim 1, recite limitations similar to those set forth above with respect to claim 1. Claims 23, 24, 29, and 36 are therefore allowable for at least the reasons presented above with regard to claim 1. Claims 25-28 and 30-35 are also allowable at least due to their dependence from claims 24 and 29 respectively.

II. Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Application No. 09/759,100
Attorney Docket No. 96-3-512CON1CP2
Customer No. 32,127

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 07-2347.

Respectfully submitted,

VERIZON CORPORATE SERVICES GROUP INC.

Dated: June 8, 2006

By: _____
Joseph R. Palmieri
Reg. No. 40,760

Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code: HQE03H14
Irving, Texas 75038
972-718-4800